Governance, Risk & Compliance (GRC) Software – An Exploratory Study of Software Vendor and Market Research Perspectives

Nicolas Racz  
TU Vienna  
racz@ifs.tuwien.ac.at

Edgar Weippl  
TU Vienna  
eweippl@ifs.tuwien.ac.at

Andreas Seufert  
Steinbeis Hochschule Berlin  
andreas.seufert@i-bi.de

Abstract

The integration of governance, risk, and compliance (GRC) activities has recently witnessed increased attention. Many organizations have deployed integrated GRC software. In this paper scientific research examines state-of-the-art GRC software for the first time in answering two questions: What is state-of-the-art GRC software according to the software industry, and how should scientific research deal with it? Through a survey among GRC software vendors and a comparison with existing GRC software frameworks from market research we derived eight findings. While software vendors share a common basis in their GRC understanding, they deliver diverse functionality. Market research frameworks have different scopes and they do not match the vendors’ perceptions. The products’ technology architectures mainly differ in their degree of integration, which is a key topic in future developments. Due to the lack of congruence, industry perspectives and existing state-of-the-art GRC software should only very cautiously be applied in research.

1. Introduction and motivation

The last decade has seen increased turbulence in the economy. The crash of the dot-com bubble in 2001 and the current global financial crisis have demonstrated the instability of markets and of the global financial system [1]. Globalization has increased competitive pressures for companies. Corporate fraud scandals, environmentalism and other factors have triggered the suggestion and introduction of many new high-impact regulations [2, 3] such as the Sarbanes-Oxley-Act of 2002 and Basel II. One of the effects of these developments is the growing complexity of three disciplines: corporate governance, risk management, and compliance.

Corporate governance deals with internal and external aspects of an organization [4]. It can be understood as “involving a set of relationships between a company’s management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined” [5]. The bankruptcies of companies such as Enron, Worldcom, Parmalat and – more recently – Lehman Brothers are widely attributed to a lack or failure of corporate governance in these companies that led to balance sheet manipulations and risky adventures putting the companies’ existence at stake [6].

Governance is often supported by an organization-wide risk management system. A widely accepted definition of enterprise risk management (ERM) was published by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). Thus ERM “is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of objectives” [7].

Compliance generally describes processes that assure the adherence of an organization to regulatory, legal, contractual and other obligations.

The increasing number of laws and regulations, the increased risks that organizations have to deal with, and the growing governance concerns have induced companies, consultancies, auditing companies and software vendors to rethink conventional, separated approaches to governance, risk management, and compliance [8]. An integrated approach to the three disciplines was first described in 2004 [9] and is commonly referred to as “GRC”. Since then the acronym has rapidly penetrated the world of business and information technology (IT). GRC is used to label service offerings, departments, and particularly software products. Many companies turn to software to help automate their GRC efforts [10].

A recently published literature review found that the term GRC is primarily promoted by software
vendors. The authorship of 40 out of 107 reviewed publications could be attributed to one of the many technology providers. Their perspective on GRC is a driving force in today’s GRC domain with a strong impact on the public perception of the topic [11]. At present research lags behind the industry. Scientific recommendations for the architecture or functionality of GRC software have not been made, and the functionality involved in integrated GRC suites has not yet been scientifically identified. An analysis of what the GRC software industry puts under the umbrella of “GRC” could provide a good starting point for the research of GRC technology.

Therefore this research was carried out in order to answer two questions:

1. What is state-of-the-art GRC software from the viewpoint of software vendors, market analysts and other organizations in the industry specializing on GRC?

2. What are the implications of the software industry’s perspectives for scientific research?

2. Research methodology

The methodology applied in the research at hand consists of four stages. First we reviewed existing scientific and market research containing GRC software classifications and frameworks. Section three provides an overview of the sources identified.

In a second step we conducted a survey among vendors of GRC software suites. The survey was limited to ten questions in order to increase the probability of participation. The questions were developed drawing on our understanding of GRC gained in a prior research project that provided a GRC short-definition and a frame of reference for research of integrated GRC [11]. The questions can be subsumed under three main categories: two questions about the vendors’ understanding of GRC in general, five questions about the vendors’ present GRC software portfolio, and three questions about the vendors’ future GRC software portfolio. The whole questionnaire is available for download at www.grc-resource.com/grc_vendor_survey.pdf.

For selection of respondents we wanted to focus on providers of “integrated GRC management suites”, i.e. vendors that try to offer solutions covering as many aspects of governance, risk, and compliance management as possible. Vendors of point solutions such as pure risk management software were not in scope. Therefore we based our selection on the vendor list of the 2008 Gartner Magic Quadrant for Enterprise Governance, Risk and Compliance Management [12] and added further vendors that claimed to provide integrated GRC solutions. The resulting 27 companies were contacted through email and asked for participation several times. Eventually eight vendors returned answers, a response rate of 30%. One set of answers had to be disregarded because its quality was insufficient. The participants taken into consideration were CA, IDS Scheer, MetricStream, Protiviti, SAP, Thomson Reuters, Wolters Kluwer, and Paisley (which has meanwhile been acquired by Thomson Reuters).

The answers sent to us were prepared by heads of product development or portfolio managers from marketing. Where responses were unclear we contacted the vendors again and clarified the issues. Depending on the nature of the topic, answers were processed in different ways in order to find common or distinguishing elements (see table 1).

<table>
<thead>
<tr>
<th>Questions</th>
<th>Evaluation Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1: GRC definition</td>
<td>Decomposition of GRC short-definition into twelve components; comparison of congruence with vendor answers; calculation of percentage of congruence;</td>
</tr>
<tr>
<td>Q2: GRC and ERM</td>
<td>Qualitative analysis</td>
</tr>
<tr>
<td>Q3: GRC portfolio</td>
<td>Standardization of wording; exclusion of non-functional features following the classification of Roman [13]; statistical analysis of functionality mentioned; resulted in 35 different functional capabilities, not counting regulation- or methodology-specific modules (e.g. ISO9000 or Six Sigma); statistical analysis</td>
</tr>
<tr>
<td>Q5: Unique selling point</td>
<td>Answers not used in this research</td>
</tr>
<tr>
<td>Q6: Customer benefits</td>
<td>Standardization of wording; statistical analysis</td>
</tr>
<tr>
<td>Q7: Centralization</td>
<td>Qualitative analysis</td>
</tr>
<tr>
<td>Q8,9,10: Future trends</td>
<td>Qualitative analysis</td>
</tr>
</tbody>
</table>

In the third stage we brought together the results from the survey with a deeper analysis of the existing frameworks identified in the first step in order to see in how far the views on GRC software of software vendors are congruent with those of market research and other organizations. We identified eight key findings that are the primary result of our research. Figure 1 gives an overview of the research structure, depicting which findings (F1...F8) were derived from which answers to the survey questions (Q1...Q10) and from the analysis of existing models. The findings are described in section four.

In the fourth stage the implications of the findings for scientific research were discussed. They are presented in section five.
3. Prior research

So far research on GRC software has only been carried out as typical technology market research by Gartner Research, Forrester Research and AMR Research, and by the Open Ethics and Compliance Group (OCEG) that provides a framework for GRC information technology.

Gartner defined a “Comparison Model for the GRC Marketplace” [14]. It is applied in the yearly composition of the “Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms” that evaluates and ranks vendors’ GRC portfolios. Gartner identifies four primary functions of enterprise-wide governance, risk, and compliance platforms: audit management, compliance management, risk management, and policy management [12, 15].

A similar study is regularly provided by Forrester Research as “The Forrester Wave: Enterprise Governance, Risk and Compliance Platforms” [16]. The functional categories of GRC platforms as identified by Forrester are policy and procedure management, risk and control management, event and loss management, and GRC management and analytics. Furthermore Forrester considers “technical functionality” in the areas of content management, process management and project management, but the category also includes non-functional criteria such as scalability, usability, configurability, flexibility and ability to integrate.

AMR Research published a GRC framework in 2008. Through a mix of general research and vendor evaluation they developed a GRC taxonomy consisting of three categories: GRC management software, GRC execution capabilities, and GRC applications that “address specific business processes as identified by regulatory agencies across the globe or industry-led consortia that may or may not incorporate specific GRC management and/or execution components” [17]. GRC management applications comprise risk and control frameworks (e.g. policies), risk management software, dashboards and reporting, as well as initiative-specific content. Access controls and identity management products, business process controls, audit testing tools and data security products are part of the GRC execution category. GRC applications are a myriad of products managing specific issues (e.g. environmental health and safety, global trade management or IT risk management). The category is not defined in more detail.

Since AMR only publishes vendor profiles one-by-one, they can adapt their framework in a flexible manner for each vendor analysis, while Gartner and Forrester are forced to confine the GRC platform more strictly. As AMR Research was acquired by Gartner in 2009, it is not sure if its current framework will remain in use.

The same market research companies also provide high-level research of GRC software portfolios in general, e.g. “The Enterprise Governance, Risk and Compliance Platform Defined” by Gartner [18] or “The GRC Technology Puzzle: Getting All The Pieces To Fit” by Forrester [19]. An older framework for GRC software has been provided by Rasmussen for Forrester Research [20]. It consists of four levels. The lowest layer is the supporting technology infrastructure software. Financial risk software and operational risk and control software constitute the second level. The third level consists of the GRC platform, including policies, procedures and controls, risk and control assessment, risk analytics and loss, events and investigations management. Enterprise risk management dashboards on the fourth level complete the framework. On request however Rasmussen stated that this model is now deprecated.

The market research models are useful for the purpose of ranking products of a clear-cut, delimited hypothetical market, but they aggregate functionality on a level that is too high to enable deeper analysis for scientific research purposes without access to internal methodology documentation. The results of software vendor rankings differ depending on which research company’s framework and methodology is used, underlining the differing composition and priorities of the models applied. Without further ado it is not possible to say if one of the frameworks is more or less valid than the others. Being deprived of the research companies’ documentation, scientific research can only determine the common and distinguishing elements of the various frameworks.

A more exhaustive and detailed classification of GRC software is provided by the non-profit organization “Open Compliance and Ethics Group” (OCEG) in its “GRC-IT Blueprint” [21]. OCEG lists 72 GRC software applications, which they call
“technology modules”. These are mapped to one of three “technology levels” as well as to one of nine “technology arenas”. The technology levels are (software) infrastructure, business applications, and GRC specific applications. The nine technology arenas consist of corporate governance, assurance and audit management, business intelligence, business process management, enterprise content management, enterprise resource management, human resources management, security management and risk management.

The OCEG model is more detailed than the market research frameworks. Also professionals from various organizations were involved in its creation. However it shares some deficits with the market research frameworks. They all lack transparency and their scientific validity is not verifiable as the methodology that led to their construction has not been published. Moreover as the frameworks are not openly accessible their application is restricted to a small community of users that is able and willing to pay for the reports. The different GRC perspectives presented inhibit the development of a common understanding of integrated GRC software suites and their components.

Despite these shortcomings the frameworks could theoretically still be useful for research as a basis for a first identification of GRC software. The whole of the functionality mentioned could give an indication about components possibly enabling integrated GRC; common elements might indicate a higher importance of certain functionality over other components. So far an identification of the frameworks’ common elements has not been conducted. Therefore in this research the existing frameworks were compared and in addition matched against the software vendors’ perspectives on GRC as provided through our survey.

4. Results

Our study delivered eight key findings.

4.1. F1: Software vendors share a common basis in their understanding of GRC.

In order to ensure comparability of survey answers it was important to see if participants followed the idea of integrated GRC as we see it to a sufficient extent. For this purpose we matched the vendor definitions against the as of today sole scientifically derived short-definition of GRC [11]: “GRC is an [integrated, holistic] approach to [organization-wide] governance, risk and compliance ensuring that an organization [acts ethically correct] and in accordance with its [risk appetite], [internal policies] and [external regulations] through the alignment of [strategy], [processes], [technology] and [people], thereby improving [efficiency] and [effectiveness].”

At average 58% of the definition’s twelve components (marked in square brackets) were matched in vendors’ definitions, with a standard deviation of 14.4%. The largest congruence was found to be 75%, the smallest 42%. The median of 58% matches the average exactly. The aspects most rarely included were people (once), ethics and efficiency (twice each). Integration was mentioned explicitly by all vendors but one, who mentioned it implicitly. The integrated approach to GRC is the key prerequisite to enable a comparison of the participants’ answers.

The congruence of vendors’ GRC definition with the definition applied in this research is sufficiently high to allow for a purposeful analysis. Vendors are sharing a common basis in their definition of the term GRC.

4.2. F2: Software Vendors see the relation of GRC and Enterprise Risk Management in two different ways

The relation of GRC and Enterprise Risk Management (ERM) has been discussed briefly by Banham [22], who concluded that there were different perceptions. Our survey identified two different viewpoints of the GRC-ERM-relation. Either ERM and all of its components (such as risk identification, risk assessment, risk monitoring, etc) are considered a part of GRC (P1 in figure 2); or ERM and GRC are seen as interconnected, partially overlapping methodologies that share certain processes and technologies enabling these processes (P2). Consequently in the first case processes exclusive to ERM are classified as being part of GRC, whereas the second perspective puts them outside the GRC domain.

![Figure 2. The two perceptions of the GRC-ERM relation](image)

In order to see if participants followed the idea of integrated GRC as we see it to a sufficient extent. For this purpose we matched the vendor definitions against the as of today sole scientifically derived short-definition of GRC [11]: “GRC is an [integrated, holistic] approach to [organization-wide] governance, risk and compliance ensuring that an organization [acts ethically correct] and in accordance with its [risk appetite], [internal policies] and [external regulations] through the alignment of [strategy], [processes], [technology] and [people], thereby improving [efficiency] and [effectiveness].”
In our survey four companies supported the first perspective, while three stated that ERM and GRC only shared a number of common elements. For vendor CA, for instance, GRC is the unification of ERM and compliance. Protiviti notes that definition-wise GRC and ERM are very similar, but market practices show the actual difference: They claim that GRC typically encompasses a broader spectrum of activities associated with managing an organization while ERM has tended to be more focused on a subset of activities and processes to manage risks within an organization.

4.3. F3: Vendors’ perceptions of GRC functionality are diverse

Vendors have different perspectives on which functionality should be delivered by GRC software. We asked vendors to list the functional capabilities of their GRC portfolios. The answers were harmonized as different wording was often used to describe the same or strongly overlapping functionality, e.g. risk management and enterprise risk management, or event management, issue management and incident management. We built groups of overlapping and synonymous functionalities where possible.

Harmonization resulted in a list of 35 high-level functionalities. Only 13 were named by more than one vendor.

**Table II. GRC software functionality named by more than one vendor**

<table>
<thead>
<tr>
<th>Function</th>
<th># times mentioned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk management (RM, ERM)</td>
<td>7</td>
</tr>
<tr>
<td>Policy management</td>
<td>7</td>
</tr>
<tr>
<td>Audit management</td>
<td>7</td>
</tr>
<tr>
<td>Reporting / dashboards / analytics</td>
<td>7</td>
</tr>
<tr>
<td>Case / issue / event / remediation / loss management</td>
<td>6</td>
</tr>
<tr>
<td>Operational risk management</td>
<td>5</td>
</tr>
<tr>
<td>Compliance management</td>
<td>5</td>
</tr>
<tr>
<td>Controls testing and management</td>
<td>4</td>
</tr>
<tr>
<td>Financial controls</td>
<td>3</td>
</tr>
<tr>
<td>Surveys</td>
<td>3</td>
</tr>
<tr>
<td>Workflow management</td>
<td>3</td>
</tr>
<tr>
<td>Corporate governance</td>
<td>2</td>
</tr>
<tr>
<td>IT audits and compliance</td>
<td>2</td>
</tr>
</tbody>
</table>

The vendor mentioning the fewest components came up with seven items. For one vendor we counted 15 items even after harmonization. The average vendor listed 11.86 different GRC capabilities (median: 12) with a standard deviation of 2.67 items. At average each capability was named in 2.37 out of the seven answers with a standard deviation of 2.16. Consequently there is a rather low degree of congruence. Vendors share a common core of GRC capabilities, but apart from the core the GRC functionality offered is very vendor specific.

22 capabilities were only mentioned once each: program and project management, corporate social responsibility, training management, quality management, nonconformance management, supplier quality management, GRC management, configuration management, document management, role-based security, risk and control assurance, IT governance, IT GRC, supply chain risk and compliance management, global trade management, environmental services, testing and documentation, sign-off management, mapping of policies, risks and controls with processes and hierarchies, internal control system definition, documentation and publication, and fraud detection.

4.4. F4: The scope of existing GRC software frameworks varies strongly

In order to compare the three frameworks from technology market research as described above, they were mapped and classified using the AMR categorization of GRC management, execution, and application software. To a large extent the components described in the frameworks overlap.

**Table III. Comparison of market research GRC frameworks**

<table>
<thead>
<tr>
<th>GRC management</th>
<th>AMR</th>
<th>Forrester</th>
<th>Gartner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk and control framework</td>
<td>Policy and procedure management</td>
<td>Policy management</td>
<td>Compliance management</td>
</tr>
<tr>
<td>Risk management software</td>
<td>Risk and control management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dashboards and reporting</td>
<td>GRC management and analytics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(non-functional: Initiative-specific content)</td>
<td>Event and loss management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The functional classification of Forrester and Gartner focuses on GRC management capabilities. This confinement makes sense in two ways. Firstly, it helps draw clean lines between GRC solutions and other product lines such as business intelligence or enterprise content management that support GRC but also other disciplines (even though the GRC analytics included by Forrester represent an exception). Secondly, assuming an integrated GRC process the management functions are the capabilities most likely to be integrated on a single platform, or even in a single application, in order to deliver a central management tool providing an overview of GRC activities.

The scope of the AMR classification is wider than that of Gartner and Forrester, especially in the GRC execution and application categories, thus going beyond GRC management capabilities.

The OCEG GRC-IT Blueprint with its 72 technology modules is even more comprehensive and granular, to an extent that a one-to-one mapping to the market research classifications is not convenient. The OCEG category “GRC specific applications” covers many of the GRC management capabilities as identified by market research. This category consists of 30 modules covering compliance and governance, different types of controls, risk management and audit applications, and further modules such as accountability management, crisis management, discovery, helpline and hotline, legal matter management and more.

The main difference between the OCEG model and the three market research models is the list of 24 business applications that includes basically all applications somehow relevant for GRC, such as knowledge management, customer relationship management, budget and finance management, and project portfolio management. The OCEG infrastructure category contains some of the GRC execution capabilities of the AMR model – access control, identity management and data security products – but not audit tools and business process controls, which for OCEG are GRC specific applications. Other infrastructure functionality such as system logs management and physical security is OCEG specific, as it is not mentioned in the market research models.

In summary it can be stated that while certain elements (GRC management and audit management) exist in all frameworks, the scope of the four frameworks analyzed varies strongly.

4.5. F5: Vendors’ understanding of GRC software functionality differs from existing frameworks

The 35 GRC software modules overall and the 11.86 functionalities average named by vendors are a lot more than listed by technology research companies. Consequently the GRC scope of most vendors clearly surpasses the scope outlined in the technology market research reports. The common ground of vendors and market research are the GRC management capabilities and audit management.

Compared to the OCEG GRC-IT Blueprint with its 72 technology modules, vendors’ portfolios are much more delimited in scope. The deviation exists for several reasons.

Partly this is owed to the fact that the nine infrastructure technology modules identified by OCEG are hardly mentioned by the participants of our survey (IT operations management, physical security, enterprise architecture standards or configuration and change management, among others); apart from access controls, vendors do not seem to refer to this functionality as being delivered by GRC software.

Another reason is granularity; a vendor application can comprise more than one OCEG technology module while carrying only a single name; for instance “Operational Risk Management” in the vendor’s understanding may already include the separate OCEG module “Risk Analytics”. “Operational Assurance & Audit”, “Information Technology Audit” and “Audit Analytics” may be subsumed under “Audit Management”, etc.

Furthermore, some of the items in the OCEG business applications category are simply not considered to be “GRC” by vendors. Capabilities for transaction management, corporate performance management, email management or customer relationship management are actually offered by some vendors, but were not included in the survey answers. However this does not apply to all the OCEG business applications; vendors count loss management, learning & training management, document management and
other modules towards their GRC portfolio. However, apart from loss management and dashboards, none of these OCEG business applications was mentioned by more than one vendor.

With “news feeds”, OCEG also lists content, which we do not consider in this part of our study; with “helpline”, “hotline/whistleblower” and “physical security” it includes items that are generally not software applications in the first place.

It can be concluded that vendors at average have a broader definition and portfolio of GRC software than technology market research companies, but a more confined perspective than that described by OCEG. Vendors’ understanding of GRC software functionality therefore differs from existing frameworks.

4.6. F6: Vendors agree on the benefits delivered through integrated GRC suites to a large extent

Respondents were asked for the top five benefits their customers normally gain when employing their GRC solution. Of course the answers might be marketing-driven and they might not reflect the actual outcomes of GRC implementations, but they still show which benefits customers are trying to achieve, as these benefits are explicitly addressed by vendors.

The wording of the answers strongly varied, but the gist of the statements was in most cases found to belong to one of four categories: better transparency (6x), increased efficiency (6x), improved risk management (5x), and reduced costs (5x). Other benefits mentioned included streamlining the organization through centralization (2x), alignment (2x), competitive advantage (1x) and increased agility (1x). Sometimes two benefits listed by a vendor could be attributed to the same category, hence the reduction of the number of references in sum from 35 to 28.

The result implies that the promoted customer benefits of GRC are universal, being mentioned by most of the vendors. The benefits seem to be relatively tool independent, lying in the nature of the integrated GRC approach and in commonalities of the GRC platforms.

4.7. F7: Technology architectures of vendors mainly differ in their degree of integration

The technology architecture descriptions we received varied strongly in detail. Still the information provided was sufficiently comparable to conclude that – programming languages and other implementation details left aside – the main technological difference between vendors’ architectures is the degree of integration. Integration aspects are found on six levels.

1) Technology infrastructure: Is the GRC software open to many platforms and can it share resources, also with other product lines? Are there hardware or database restrictions? Does complexity of the technology infrastructure increase when more GRC modules of a vendor are added because they have differing technology infrastructure requirements?

2) Data model and data store: Are GRC modules sharing a data model wherever it makes sense? Is structured and unstructured data (documents, comments) combined and saved in a single data store?

3) Integration with ERP systems and other relevant non-GRC software: How easily can GRC applications integrate data from other systems? Can they directly influence the process flow in these systems, for instance through direct application and execution of rules provided by GRC?

4) Coherent reporting: Do the tools enable GRC reporting together with reporting of conventional performance data?

5) Front-end environment: Does the user experience a single environment for the various GRC applications (single sign-on, joint presentation in a portal or the like)?

6) Front-end look and feel: Are navigation and user interface elements reasonably harmonized across GRC tools?

The integration possibilities might be one of the key enablers of GRC benefits through reduction of costs and human resources, through shortened process cycle times and improved data and process quality.

4.8. F8: Five key trends influence GRC technology in the near future

Based on the survey answers five key trends were identified that, according to vendors, influence the future development of GRC technology.

1) Integration of GRC with business processes: As SAP states, “GRC is not an external, 'end of process' or check the box activity, and must be integrated into the performance of a business process in order for companies to receive the greater value of GRC.” Integration of GRC with business processes supports the trends towards continuous monitoring and involvement of more and more people in GRC activities. [23, 24]. IDS Scheer also focuses on the aspect of business process driven GRC.

2) Integration of GRC with performance management: Understood as a closed-loop model for managing the planning, monitoring and controlling of business processes and their performance within BPM
it is obvious that performance management will gradually be merged with GRC as a result of the integration of GRC with business processes. The key link between performance management and GRC is risk. Business risks will be considered in the planning process; they need to be monitored; and key risk indicators complement key performance indicators when deciding about control measures.

(3) Continued integration of GRC software on a single technology platform: With specialist vendors enhancing their portfolio to cover more GRC functionality on the one hand, and ERP vendors and consultancies penetrating into the market on the other hand, GRC includes a myriad of software components. Market consolidation is still in its early stages. Efforts to provide more coherent, integrated platforms are ongoing.

(4) Centralization of GRC-relevant information: The precedent trend of reducing technological complexity supports another trend: bringing together GRC-relevant information. Data warehouses historically have struggled to integrate unstructured data. Risk management is mostly carried out as a function separated from performance management, resulting in data silos. Enterprise-wide consistent document management in many companies still has not been realized. GRC-relevant information from all included activities needs to be merged, the different types of data need to be connected, and the whole needs to be presented in a seamless manner. According to CA, for example, the centralization of risk and compliance information is important in order to eliminate redundancies.

(5) Improved analytics and reporting: In general vendors seem unsatisfied with current reporting and analytics solutions. Owed to the complexity of merging applications that have been managed separately so far, reporting silos still exist and analytics do not dig as deep and work as efficiently as desired. Thomson Reuters states that consistent reporting across the various disciplines of GRC should be a decisive feature of an integrated GRC suite.

5. Discussion and implications for research

The survey response rate of 30% is considered to be high, given that answering the survey must have taken several hours judging from the length of the responses. The high degree of participation shows the interest of vendors both to promote their own perspective on GRC and to learn more about the viewpoints of competitors.

Of course there are points of critique that can be brought forward against the research methodology applied. The questionnaire design with open answers enables vendors to elaborate on their GRC perspective, but it also introduces inaccuracy through different wording and focis. Vendors try to promote their products and therefore tend to highlight strengths and disregard weaknesses of their tools. We still decided to leave the questions open-ended so that vendors would not be confined to a frame that might inhibit gaining a full understanding of GRC as seen by the software industry.

Another issue is that the analysis of the answers might not always have been accurate because resource restrictions inhibited a deeper analysis of certain issues, for example in how far vendors’ policy management applications offer the same functionality. However as the survey was conducted to gain a general idea of GRC software, and not to derive an exact technology reference model in the first place, keeping the analysis at a high level does not harm the research.

Lastly the findings represent a momentary snapshot of state-of-the-art software that will change over time. The young GRC market is in an early phase of consolidation. Recent market activity includes the acquisition of Paisley through Thomson Reuters and of Archer Technologies through EMC. The spectrum of GRC tools is still immense. One of the ideas behind integrated GRC is to reduce complexity in processes, but the merger of more and more products in GRC suites and the integration of acquired products are going to increase complexity of the technology applied. Vendors progress with product integration on the integration levels described above. Some vendors have come far on this path because they rely on a GRC platform that has been built from the scratch, while others have more complex technology architectures due to integration challenges of diverse tools. But even vendors with advanced integration between the three disciplines face another integration challenge while GRC moves closer towards business process execution.

Aware of the possible deficits of the research at hand, what are the implications of the eight findings to scientific GRC research in general?

In the case of F2, we recommend the first perspective, with ERM being completely contained in GRC, to be adopted by GRC researchers. Otherwise they run the risk of excluding processes that bear potential for integration with other disciplines within GRC today or in the future.

F3, F4 and F5 show that the various vendors, market research companies and OCEG all have different perspectives on GRC. The common basis that vendors share in their GRC definitions (F1) has hardly led to a shared perspective on GRC functionality. F3 and F4 demonstrate that at least GRC management (risk and policy/compliance management) as well as
audit management and reporting are counted towards GRC software functionality by the large majority of the organizations considered in this research.

We continue to deem the analysis of the status quo of GRC software as useful in order to identify gaps, to learn from errors made in the past, and to understand GRC requirements. However GRC technology research in general should not be based on the analysis of a single vendor’s GRC portfolio or a single framework. Even the small common core of the portfolios and frameworks does not provide a firm basis to be applied in scoping GRC research; it may merely help prioritize the functionality to be examined. The same can be said about F6, F7 and F8 – they may help draw the attention of researchers towards a specific set of benefits, integration possibilities and future developments, but research should not be restricted to the results of these findings.

In addition to the findings certain elements of existing perspectives could also be used as theoretical imputus, such as the AMR distinction of GRC management and GRC execution software applied in F4 that gives an apparently reasonable recommendation for segmentation of GRC software functionality. However any concepts taken over have to be scientifically validated before being applied in research.

Apart from heterogeneity another shortcoming of the existing portfolios and frameworks underlines the cautious approach that research should take when using them. The GRC software products on the market have to be sold today; therefore they have to integrate with customer landscapes. The market research frameworks are also bound to be applicable as of now, otherwise they would not sell. Thus the creators of software and market research depend on the revenue generated through their products. Consequently both software and frameworks heavily depend on the status quo in organizations. However a new, integrated approach to GRC might require change on a larger scale, on strategic, organizational, process and technology levels. New information technology concepts might have to be applied.

To sum it up, research of GRC software should follow one of the “classic” procedures of software engineering [26]. It should start with the identification of organizations’ current and foreseeable future GRC requirements. Then GRC process models to cover these requirements in an integrated manner should be developed. Finally research should derive software functionality and an adequate architecture enabling the execution of the recommended GRC processes, considering state-of-the-art and newly suggested technology from practice and research. Current GRC software does not provide a shortcut in this process.

This research followed the requirements of the information systems research framework [27]. We identified that when developing and building theories and artifacts for GRC technology, research should not rely heavily on technology present in the environment. This research further derived eight key findings that help researchers understand and approach the GRC domain, GRC software and GRC frameworks. Originality is given as for the first time technology market research frameworks were compared. Also for the first time scientific research compared the high-level functionality of state-of-the-art GRC software products to each other and to market research. A first consideration of these tools and models in the early phases of GRC research was indispensable as contemporary GRC software is used by many organizations world-wide; the frameworks of market research and OCEG are also widely used to facilitate buying decisions and to help understand and manage GRC.

6. Conclusion and future research

The research presented was carried out in order to find out about state-of-the-art GRC software and its implications on scientific research. As has been shown an understanding of software vendors’ GRC products and of existing GRC models can provide valuable insights, but due to the different perspectives on GRC in the industry future research should not be based purely on such an analysis. We recommend constructing a reference model for integrated GRC software based on scientifically applied software engineering.

For our share we will focus on GRC management processes for information technology operations. By means of an analysis of frameworks and best practices we will construct a process model for IT GRC management before deriving software functionality and an IT architecture that can provide support to the processes in scope. To close the loop, the tools of software vendors can then be mapped to the resulting reference model in order to identify gaps between contemporary GRC practice and its real potential.

7. References


